Finite Fields and Their Applications 18 (2012) 434–436

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

An alternative proof of a result on the weight divisibility of a cyclic code using supersingular curves

Gary McGuire [1]

School of Mathematical Sciences, University College Dublin, Ireland

ARTICLE INFO

Article history:
Received 23 June 2011
Revised 13 September 2011
Accepted 29 September 2011
Available online 19 October 2011
Communicated by Xiang-dong Hou

MSC:
94B15
14H45

Keywords:
Supersingular curve
Cyclic code
Divisibility

ABSTRACT

We present an alternative proof of a result of Zeng–Shan–Hu that shows that the cyclic code with three zeros α, α^3, α^{13} has the same weight distribution as the 3-error-correcting BCH code. Our proof uses the theory of algebraic curves over finite fields, and combines results that are already in the literature. This method is applicable in other cases too.

1. Introduction

Let α be a primitive element in the finite field $\mathbb{F}_q$, where $q = 2^n$. The binary cyclic code of length $2^n - 1$ with three zeros α, α^3, α^5 has dimension $2^n - 1 - 3n$, and minimum distance 7, and is called the binary 3-error-correcting BCH code. If n is odd, the dual code of this BCH code is known to have five nonzero weights, and the weight distribution is known, see [2]. It is of interest to find other cyclic codes with three zeros having the same weight distribution. Recently, a paper by Zeng, Shan and Hu [5] proved that the cyclic code with zeros α, α^3, α^{13} is such a code. We refer to [5] for background and further references. Their proof used the following characterization theorem due to Hollmann and Xiang [1].

E-mail address: gary.mcguire@ucd.ie.

[1] Research supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2011.09.009

Theorem 1. *Let n be odd and let C be a binary cyclic code of length $2^n - 1$, dimension $2^n - 1 - 3n$, and minimum distance at least 7. If all weights in $C^\perp$ are divisible by $2^{(n-1)/2}$, then C has the same weight distribution as the binary 3-error-correcting BCH code of the same length.*

For the remainder of this note, let C denote the cyclic code with zeros α, α^3, α^{13}. In order to apply Theorem 1, the authors of [5] showed

(i) that C has minimum distance 7, and
(ii) that all weights in $C^\perp$ are divisible by $2^{(n-1)/2}$.

The proof of (ii) is long, and the hardest part of the paper [5]. The purpose of this note is to give a short proof of (ii) using the theory of algebraic curves over finite fields.

2. A proof using algebraic curves

The trace description of $C^\perp$ states that all codewords in $C^\perp$ have the form

$$w_{a,b,c} = \left(\ldots, \mathrm{Tr}\left(ax + bx^3 + cx^{13}\right), \ldots\right)_{x \neq 0}$$

for $a, b, c \in \mathbb{F}_q$. The notation means that the entry in position x is $\mathrm{Tr}(ax + bx^3 + cx^{13})$. Determining the Hamming weight of a codeword is the same as determining the number of 0's in the codeword. Since elements of trace 0 have the form $y^2 + y$, knowing the Hamming weight of $w_{a,b,c}$ is equivalent to knowing the number of solutions of

$$y^2 + y = ax + bx^3 + cx^{13}. \tag{1}$$

Indeed, if N denotes the number of (projective) $\mathbb{F}_q$-rational points on the algebraic curve (1), and if W is the weight of the codeword $w_{a,b,c}$, then

$$2W = 2q + 1 - N.$$

It follows that all weights in $C^\perp$ are divisible by $2^{(n-1)/2}$ if and only if all values of $q + 1 - N$ are divisible by $2^{(n+1)/2}$, as a, b, c vary. Applying the following two theorems from the literature completes the proof of (ii).

Theorem 2 is actually a corollary of a result in [3], which characterizes divisibility of the coefficients of the characteristic polynomial of the Frobenius endomorphism of a supersingular abelian variety.

Theorem 2. *(See Stichtenoth and Xing [3].) Let $q = p^n$ where n is odd. If N is the number of projective $\mathbb{F}_q$-rational points on a supersingular genus g curve defined over $\mathbb{F}_q$, then $N - (q + 1)$ is divisible by $p^{(n+1)/2}$.*

The final result we need shows that (1) is indeed a supersingular curve.

Theorem 3. *(See Scholten and Zhu [4].) The curve $y^2 + y = ax + bx^3 + cx^{13}$ is a supersingular genus 6 curve.*

Combining Theorems 2 and 3 with the observation made above proves (ii).

The proofs of Theorems 2 and 3 require a careful analysis of the Newton polygon of the characteristic polynomial of Frobenius, where extra information is available in the case of a supersingular abelian variety.

We remark that this method of proving divisibility can be used for cyclic codes with other zeros. The (possible) difficulty lies in proving that the corresponding curves are supersingular. For example, the cyclic code with three zeros α, α^3, α^{11} has all weights in its dual divisible by $2^{(n+1)/2}$, because

the curve $y^2 + y = ax + bx^3 + cx^{11}$ was shown to be supersingular in [4]. Similarly for the code with two zeros α^3, α^5; the code with three zeros α^3, α^5, α^9; and for the code with four zeros α^3, α^5, α^9, α^{17}.

References

[1] H. Hollmann, Q. Xiang, On binary cyclic codes with few weights, in: D. Jungnickel, H. Niederreiter (Eds.), Finite Fields and Applications, Proceedings of Fq5, Springer, 2001, pp. 251–275.
[2] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error–Correcting Codes, North-Holland, Amsterdam, 1977.
[3] H. Stichtenoth, C. Xing, On the structure of the divisor class group of a class of curves over finite fields, Arch. Math. 65 (2) (1995) 141–150.
[4] J. Scholten, H.J. Zhu, Hyperelliptic curves in characteristic 2, Int. Math. Res. Not. IMRN 17 (2002) 905–917.
[5] X. Zeng, J. Shan, L. Hu, A triple-error-correcting cyclic code from the gold and Kasami–Welch APN power functions, Finite Fields Appl. 18 (1) (2012) 70–92.